What is claimed is:

1. A method for generating pseudo-random numbers comprising:

a first step for setting up an initial state value of a linear feedback shift register including n plurality of shift resistors and capable of outputting a bit string having bit number of (2^n)-1 per one cycle;

a second step for finding a derived value prime to the bit number per one cycle of the first linear feedback shift register based on the initial state value by means of a predetermined operation processing;

a third step for multiplying the derived value by a value obtained by multiplying the bit number per one cycle by two or more to calculate a bit number to be outputted from the linear feedback shift register;

a fourth step for outputting a bit string corresponding to the calculated bit number based on the initial state value from the linear feedback shift register;

a fifth step for taking out a bit from the output bit string every the number of the derived value to generate a new bit string;

a sixth step for reconstructing the linear feedback shift register such that the new bit string can be outputted from the resistor; and

a seventh step for generating pseudo-random numbers based on the initial state value from the reconstructed linear feedback shift register.

2. A method for generating pseudo-random numbers as defined in claim 1, wherein the initial state value is processed by Hash function to determine its Hash value to adopt a prime number most approximated to the Hash value as the derived number.

3. A method for generating pseudo-random numbers as defined in claim 1 or 2, wherein the reconstruction of the linear feedback shift resistor is carried out using Berlekamp-Massay algorithm.

4. A method for generating pseudo-random numbers as defined in any of claims 1 to 3, which further comprises a eighth step for subjecting the pseudo-random numbers generated in the seventh step to nonlinear conversion.

5. A pseudo-random number generator comprising:

a linear feedback shift register having n shift resistors and capable of outputting a bit string having bit number of (2^n)-1 per one cycle;

means for setting up an initial state value of the linear feedback shift register based on a secret key;

means for determining a derived value prime to the bit number per one cycle of the linear feedback shift register based on the initial state value by means of a predetermined operation processing;

means for multiplying the derived value by a value obtained by multiplying the bit number corresponding to one cycle by two or more to calculate a bit numbers to be outputted from the first linear feedback shift register;

means for outputting a bit string corresponding to the calculated bit number based on the initial state value from the linear feedback shift register;

means for taking out a bit from the output bit string every the num-

ber of the derived value to generate a new bit string;

means for reconstructing the linear feedback shift register such that the new bit string can be outputted from the resistor; and

means for generating pseudo-random numbers based on the initial state value from the reconstructed linear feedback shift register.

6. A pseudo-random number generator as defined in claim 5, which is further provided with means for generating a second linear feedback shift resistor having construction capable of outputting a new bit string, instead of the means for reconstructing the linear feedback shift resistor; and wherein the means for generating pseudo-random numbers generates the pseudo-random numbers based on the initial state value from the second linear feedback shift resistor.

7. A pseudo-random number generator comprising:

means for outputting a selectively used random number bit string having a predetermined bit number based on a secret key;

a random number table in which a plurality of amplified random bit strings having larger bit number than that of the selectively used random number bit string is stored;

means capable of selecting a corresponding amplified random number bit string from the plurality of amplified random number bit strings within the random number table by referring to the random number table using the selectively used random number bit string outputted from the means for outputting selectively used random number bit string; and

means for nonlinearly conversing the amplified random number bit

string selected by the means for selecting the amplified random number bit string by a nonlinear function to output pseudo-random numbers.

8. A pseudo-random number generator as defined in claim 7, which is further provided with means for generating the amplified random number bit string by a secret key given, storing the bit string in the random number table, and carrying out initial setup of the random number table.

9. A pseudo-random number generator as defined in claim 7 or 8, wherein:

the means for outputting selectively used random number table are plurally provided,

the random number table is provided to correspond to each of the means for outputting selectively used random number table,

the means for generating the amplified random number bit string selects a corresponding amplified random number bit string from the random number table by referring to the random number table corresponding to each of the means for outputting selectively used random number bit string respectively using the selectively used random number bit strings outputted from each of the means for outputting selectively used random number bit string, and

the means for nonlinearly conversing outputs pseudo-random numbers by nonlinearly conversing the amplified random number bit string selected from each of the random number tables by nonlinear function using each of the means for generating the amplified random bit string.

10. A pseudo-random number generator as defined in claim 9, wherein plural random number tables are provided corresponding to each of the means for outputting selectively used random number bit string, and

which is further provided with means for subjecting each of the amplified random number bit strings selected from each of the random number tables by the means for selecting the amplified random number bit string to exclusive-or operation every the means for outputting a selectively used random number bit string and outputting to the nonlinear conversion means.

11. A pseudo-random number generator as defined in claim 9 or 10, which is further provided with means for replacing the random number tables with each other at a predetermined time.

12. A pseudo-random number generator as defined in claim 11, wherein the means for replacing the random number tables has function of replacing the random number tables with each other every time that the means for outputting a selectively used random number bit string outputs the selectively used random number bit string required for referring to each of the random number tables.

13. A pseudo-random number generator as defined in claim 11, wherein the means for replacing the random number tables has function of generating random number for replacing random number tables having the same number as that of each of the random numbers, giving the random numbers for replacing random number tables to each of the random number tables as

a table number of random number table, and replacing order of the random number tables according to a rule predetermined based on the table number.

14. A program to be executed by a computer for generating pseudo-random numbers comprising:

means for outputting a selectively used random number bit string having a predetermined bit number based on a secret key;

a random number table in which a plurality of amplified random number bit strings having a larger bit number than that of the selectively used random number bit string are stored;

means capable of selecting a corresponding amplified random number bit string from the plurality of amplified random number bit strings within the random number table by referring to the random number table using the selectively used random number bit string outputted from the means for outputting selectively used random number bit string; and

means for nonlinearly conversing the amplified random number bit string selected by the means for selecting amplified random number bit string by a nonlinear function to output pseudo-random numbers.

15. A program to be executed by a computer as defined in claim 14, further comprising means for generating the amplified random number bit string by a secret key given, storing the bit string in a random number table, and carrying out initial setup of the random number table.

16. A program to be executed by a computer as defined in claim 14 or

15, wherein:

the means for outputting selectively used random number table are plurally provided,

the random number table is provided to correspond to each of the means for outputting selectively used random number table,

the means for generating the amplified random number bit string selects a corresponding amplified random number bit string from each of the random number tables by referring to the random number table corresponding to every each of the means for outputting selectively used random number bit string using the selectively used random number table outputted from each of the means for outputting selectively used random number bit string, and

the means for nonlinearly conversing outputs pseudo-random numbers by nonlinearly conversing the amplified random number bit string selected from each of the random number tables using each of the means for generating the amplified random number bit strings.

17. A program to be executed by a computer as defined in claim 16, wherein plural random number tables are provided every each of the means for outputting selectively used random number bit string, and

which is further provided with means for subjecting each of the amplified random number bit strings selected from each of the random number tables by the means for selecting the amplified random bit string to exclusive-or operation every the means for outputting selectively used random number bit string and outputting to a nonlinear conversion means.

18. A program to be executed by a computer as defined in claim 16 or 17, which is further provided with means for replacing the random number tables with each other at a predetermined time.

19. A program to be executed by a computer as defined in claim 18, wherein the means for replacing the random number tables has function of replacing the random number tables with each other every time that the means for outputting the selectively used random number bit strings outputs the selectively used random number bit string required for referring to each of the random number tables.

20. A program to be executed by a computer as defined in claim 18 or 19, wherein the means for replacing the random number tables has function of generating random numbers for replacing random number tables having the same number as that of each of the random numbers, giving the random numbers for replacing random number tables to each of the random number tables as a table number of random number table, and replacing order of the random number tables according to a rule predetermined based on the table number.